Matemática Discreta (GCID). 29-5-2024

- Nombre y apellidos:
- DNI:

1. **(1.25 puntos)** Enunciar y demostrar el Teorema de Euler de la aritmética.

   Solución. Teoría.

2. **(1.25 puntos)** Probar que un grafo $G = (V, E)$ es un árbol si y sólo si es conexo y $|V| = |E| + 1$.

   Solución. Teoría.

3. **(1 punto)** Sean las proposiciones p, q, y r. Probar que que si $p \vee q$, $p \vee r$, y $\neg p \wedge r \vee q$ son ciertas, entonces $q \wedge (p \vee r)$ es cierta.

   a) Usando tablas de verdad.

   b) Sin usar tablas de verdad.

   Solución. Usando tablas, veamos que la proposición P

$$((p \vee q) \wedge (p \vee r) \wedge (\neg p \wedge r \vee q)) \rightarrow q \wedge (p \vee r)$$

   es una tautología.

p	q	r	$p \vee q$	$p \vee r$	$\neg p$	$\neg p \wedge r$	$\neg p \wedge r \vee q$	$q \wedge (p \vee r)$	P
1	1	1	1	1	0	0	1	1	1
1	1	0	1	1	0	0	1	1	1
1	0	1	1	1	0	0	0	0	1
1	0	0	1	1	0	0	0	0	1
0	1	1	1	1	1	1	1	1	1
0	1	0	1	0	1	0	1	0	1
0	0	1	0	1	1	1	1	0	1
0	0	0	0	0	1	0	0	0	1

   Sin usar las tablas de verdad, razonamos de la siguiente manera. Si p es verdad, entonces $\neg p$ es falso, por lo que $\neg p \wedge r$ es falso. Así q debe ser verdad para que $\neg p \wedge r \vee q$ sea verdad. Entonces, ambas q y $p \vee r$ son verdad, por lo que $q \wedge (p \vee r)$ es cierta. Supoangamos ahora que p es falsa. Entonces q debe de ser verdad para que $p \vee q$ sea verdad. Entonces $q \wedge (p \vee r)$ es cierta al ser $p \vee r$ verdad por hipótesis.

4. **(1.5 puntos)** Se sabe que en un grupo de 1000 personas, 410 beben cerveza, 390 beben trina, 440 beben cocacola, 130 beben cerveza y trina, 110 beben cerveza y cocacola, 90 beben trina y cocacola, y 30 beben las tres bebidas. Responder razonadamente a las siguientes cuestiones.

   a) ¿Cuántas personas no beben ninguna bebida?

   b) ¿Cuántas personas beben una única bebida?

   c) ¿Cuántas personas beben trina y cocacola pero no cerveza?

Solución. Análogo al ejercicio del mismo tipo en la convocatoria de enero, cambiando nombre de bebida y añadiendo un cero al final a todas las cifras.

5. Obtener las soluciones enteras de los siguientes problemas, en caso de existir:

   a) **(1 punto)** El sistema
$$\begin{cases} x \equiv 5 (\operatorname{mod} 7), \\ x \equiv 4 (\operatorname{mod} 6), \\ x \equiv 1 (\operatorname{mod} 5). \end{cases}$$

Solución. Como 7 , 6 y 5 son copirmos dos a dos, el problema tiene solución. Tomamos $M = 7 \cdot 6 \cdot 5 = 210$ y las ecuaciones

$$\begin{cases} 30 s_1 \equiv 1 (\operatorname{mod} 7), \\ 35 s_2 \equiv 1 (\operatorname{mod} 6), \\ 42 s_3 \equiv 1 (\operatorname{mod} 5), \end{cases}$$

que se simplifican a
$$\begin{cases} 2 s_1 \equiv 1 (\operatorname{mod} 7), \\ 5 s_2 \equiv 1 (\operatorname{mod} 6), \\ 2 s_3 \equiv 1 (\operatorname{mod} 5), \end{cases}$$
de donde $s_1 = 4$, $s_2 = 5$ y $s_3 = 4$. La menor solucién entera positiva será entonces

$$x = (5 \cdot 4 \cdot 30 + 4 \cdot 5 \cdot 35 + 1 \cdot 4 \cdot 42) (\operatorname{mod} 210) = 208,$$

y las soluciones enteras de la forma

$$x = 208 + 210k, \ k \in \mathbb{Z}.$$

   a) **(1 punto)** La ecuación
$$8x + 17y = 2.$$

Solución. Como $\gcd(8, 17) = 1$, el problema tendrá solución. Para calularla, planteamos la ecuación
$$17y \equiv 2 (\operatorname{mod} 8),$$
o equivalentemente
$$y \equiv 2 (\operatorname{mod} 8),$$
por lo que
$$y = 2 + 8k, \quad k \in \mathbb{Z}.$$
Sustituyendo en la ecuación original

$$8x + 17 (2 + 8k) = 2,$$

de donde
$$x = -4 - 17k, \quad k \in \mathbb{Z}.$$

6. **(1 punto)** Experimentalmente se prueba que con suficiente comida, el número x_n de escarabajos lucanus cervus en el día n sigue la regla

$$x_{n+1} = x_n + 2x_{n-1}.$$

Si había un escarabajo el primer día y tres el segundo ($x_0 = 1$, $x_1 = 3$), averiguar cuántos tendremos trascurridos 101 días (dejad indicado el resultado).

Solución. Tomamos la ecuación característica

$$r^2 - r - 2 = 0,$$

con soluciones $r = -1$ y $r = 2$, y planteamos la solución general

$$x_n = A(-1)^n + B2^n,$$

con A y B constantes a determinar. De las condiciones iniciales obtenemos el sistema

$$\begin{cases} x_0 = 1 = A + B, \\ x_1 = 3 = -A + 2B, \end{cases}$$

de donde $A = -1/3$ y $B = 4/3$. Entonces

$$x_n = -\frac{1}{3}(-1)^n + \frac{4}{3}2^n$$

y

$$x_{101} = -\frac{1}{3}(-1)^{101} + \frac{4}{3}2^{101} = \frac{1}{3} + \frac{4}{3}2^{101}.$$

7. **Ejericio para recuperar las prácticas.** Utilizando el código RSA explicado en el manual de prácticas se ha enviado los cuatro números del pin de una tarjeta de crédito dígito a dígito. Sabiendo que los primos son $p = 5$ y $q = 7$ y que se ha codificado con el número $d = 5$, calcular utilizando el algoritmo de Euclides extendido, el número necesario para desencriptar 32-33-10-1 y escribir los cuatro números del pin.

Solución. El decodificador será el inverso de d en $\mathbb{Z}_m$, $m = 24$. Aplicando el algoritmo de Euclides extendido

$$\begin{pmatrix} 5 & 1 & 0 \\ 24 & 0 & 1 \end{pmatrix} \underset{F_2-4F_1}{\longrightarrow} \begin{pmatrix} 5 & 1 & 0 \\ 4 & -4 & 1 \end{pmatrix} \underset{F_1 \times F_2}{\longrightarrow} \begin{pmatrix} 4 & -4 & 1 \\ 5 & 1 & 0 \end{pmatrix} \underset{F_2-F_1}{\longrightarrow} \begin{pmatrix} 4 & -4 & 1 \\ 1 & 5 & -1 \end{pmatrix},$$

de donde por el Teorema de Bezout, tenemos que

$$1 = 5 \cdot 5 + (-1) \cdot 24,$$

por lo que $d^{-1} = 5$. Tomando $n = 35$, para decodificar el mensaje escribimos

$$\begin{aligned} 32^5 (\operatorname{mod} n) &= 2, \\ 33^5 (\operatorname{mod} n) &= 3, \\ 10^5 (\operatorname{mod} n) &= 5, \\ 1^5 (\operatorname{mod} n) &= 1. \end{aligned}$$